

Test design document for the technology demonstration of the Joint Network Defence and Management System (JNDMS) Project

Prepared by:

Eric Widdis

MacDonald Dettwiler and Associates Ltd.

Suite 60, 1000 Windmill Rd.

Dartmouth NS B3B 1L7

PWGSC Contract Number:

W7714-040875/001/SV

DID SD 003

Contract Scientific Authority:

Marc Gregorie, Project Manager (Contact Maxwell Dondo 613-998-2073)

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of the Department of National Defence of Canada.

Contract Report

DRDC-RDDC-2014-C148



**DN0656: 25 OCTOBER 2005
ISSUE 1/2: XX OCTOBER 2006**

TEST DESIGN DOCUMENT

FOR THE

**TECHNOLOGY DEMONSTRATION OF THE JOINT NETWORK
DEFENCE AND MANAGEMENT SYSTEM (JNDMS) PROJECT**

CONTRACT NO. W7714-040875/001/SV

DID SD 003

PREPARED FOR:

**DEFENCE R&D CANADA – OTTAWA
3701 CARLING AVENUE
OTTAWA ON K1A 0Z4**

PREPARED BY:

**MACDONALD DETTWILER AND ASSOCIATES LTD.
SUITE 60, 1000 WINDMILL RD.
DARTMOUTH NS B3B 1L7**

DOCUMENT APPROVAL SHEET

TEST DESIGN DOCUMENT

FOR THE

**TECHNOLOGY DEMONSTRATION OF THE JOINT NETWORK
DEFENCE AND MANAGEMENT SYSTEM (JNDMS) PROJECT**

CONTRACT NO. W7714-040875/001/SV

DID SD 003

MACDONALD DETTWILER AND ASSOCIATES LTD.

Eric Widdis _____
Author _____ (Signature) _____ (Date)

Troy Kennedy _____
Quality Assurance _____ (Signature) _____ (Date)

Brett Trask _____
Deputy Project Manager _____ (Signature) _____ (Date)

CHANGE RECORD

TABLE OF CONTENTS

1 INTRODUCTION	1-1
1.1 PURPOSE	1-1
1.2 SCOPE	1-1
1.3 DOCUMENT STRUCTURE.....	1-2
2 DOCUMENTS.....	2-1
2.1 APPLICABLE DOCUMENTS.....	2-1
2.2 REFERENCE DOCUMENTS.....	2-1
3 TESTING OVERVIEW.....	3-1
3.1 SYSTEM TESTING OBJECTIVES	3-1
3.2 JNDMS TESTING.....	3-1
3.3 JNDMS TESTING ENVIRONMENT	3-2
3.4 TEST DATA	3-5
4 TESTING ACTIVITIES AND EVENTS	4-1
4.1 UNIT TESTING	4-1
4.2 INTEGRATION	4-1
4.3 EXPERIMENTS.....	4-2
4.4 JNDMS Ad-HOC DEMONSTRATIONS	4-2
4.5 JNDMS TRIALS	4-3
4.6 JNDMS FORMAL DEMONSTRATIONS	4-3
5 TESTING METHODOLOGY AND EXECUTION.....	5-1
5.1 UNIT TESTING	5-1
5.2 INTEGRATION TESTING	5-1
5.3 EXPERIMENTS.....	5-2
5.4 JNDMS TRIALS	5-3
5.5 JNDMS DEMONSTRATIONS	5-4
6 RESOURCES, SCHEDULE AND DELIVERABLES.....	6-1
6.1 UNIT TESTING	6-1
6.1.1 Resources.....	6-1
6.1.2 Schedule.....	6-2
6.1.3 Deliverables	6-2
6.2 INTEGRATION TESTING	6-2
6.2.1 Resources.....	6-2
6.2.2 Schedule.....	6-3
6.2.3 Deliverables	6-4
6.3 EXPERIMENTS.....	6-4
6.3.1 Resources.....	6-4
6.3.2 Schedule.....	6-5
6.3.3 Deliverables	6-6
6.4 TRIALS	6-6
6.4.1 Resources.....	6-6
6.4.2 Schedule.....	6-8
6.4.3 Deliverables	6-8
6.5 DEMONSTRATIONS	6-8

6.5.1	<i>Resources</i>	6-8
6.5.2	<i>Schedule</i>	6-9
6.5.3	<i>Deliverables</i>	6-10
7	JNDMS TEST SCENARIOS	7-1
7.1	SCENARIO 1 - SYSTEM FAMILIARIZATION	7-1
7.2	SCENARIO 2 - HEADQUARTERS STAFF CHECKS NETWORK STATUS	7-3
7.3	SCENARIO 3 - ISOLATION OF A LOCAL DOMAIN	7-5
7.4	SCENARIO 4 - PHYSICAL DAMAGE	7-8
7.5	SCENARIO 5 - RESPONSE BASED ON SEVERITY OF INCIDENTS.....	7-10
7.6	SCENARIO 6 - WORKING WITH A COALITION PARTNER	7-15
7.7	SCENARIO 7 - MAINTENANCE IMPACTS USERS	7-17
7.8	SCENARIO 8 - PROVIDE NETWORK INFRASTRUCTURE DATA	7-18
7.9	SCENARIO 9 – NSM DISCOVERS AND MONITORS THE DEVICES ON THE NETWORK	7-20
7.10	SCENARIO 10 - SIM COLLECTS THE SECURITY EVENTS	7-22
7.11	SCENARIO 11 - PROVIDE MILITARY OPERATIONS DATA	7-26
7.12	SCENARIO 12 - NVAT IS INFORMED OF A NEW VULNERABILITY	7-28
7.13	SCENARIO 13 - PROVIDE SAFEGUARD DATA.....	7-31
7.14	SCENARIO 14 - MULTI-LEVEL SECURITY DOMAINS	7-32
ANNEX A - EXPERIMENTS		1
ANNEX B – TRIALS		1
ANNEX C – DEMONSTRATIONS		1

LIST OF FIGURES

Figure 1: JNDMS Development Environment	3-2
Figure 2: Network with Four Asset Locations.....	7-10

LIST OF TABLES

Table 1: Cycle 1 Workstation Configuration	3-3
Table 2: Configuration of Virtual Environments.....	3-4
Table 3: Unit Testing Personnel.....	6-1
Table 4: Integration Testing Personnel	6-2
Table 5: Experiments Personnel	6-4
Table 6: Trials Personnel	6-6
Table 7: Formal Demonstrations Personnel.....	6-8

1 Introduction

This is the Test Design Document, Data Item Description (DID) SD 003, for the Joint Network Defence and Management System (JNDMS) Technology Demonstrator (TD) project, prepared by MacDonald-Dettwiler and Associates Ltd. (MDA).

1.1 Purpose

This Test Design Document is an evolutionary document to be used to plan experiments, trials and demonstrations.

1.2 Scope

This Test Design includes:

- The test environment characteristics
- The generic scenarios to be used as baselines; it is expected that the scenarios will remain the same during the project
- The test cases associated with the system requirements; the relevant test cases will be added as functionalities of the system are detailed and developed
- A description of the modeled environment
- The actual test environment configuration to be used

This Test Design Document will include test cases, scenarios and test environment configurations applicable to:

- Unit tests
- Integration tests
- System tests
- Interface tests
- Experiments (system features tests, refer to the System Requirements Specification document [R-1] for the identification of these features)

- Trials (including acceptance tests and operational tests, involving the user community and the Defence R&D Canada [DRDC] JNDMS Project Manager [PM])
- Demonstrations

1.3 Document Structure

This document contains seven sections and four annexes, as follows:

Section 1:	Introduction
Section 2:	Documents
Section 3:	Testing Overview
Section 4:	Testing Activities and Events
Section 5:	Testing Methodology and Execution
Section 6:	Resources, Schedule and Deliverables
Section 7:	JNDMS Test Scenarios
Annex A:	Experiments
Annex B:	Trials
Annex C:	Demonstrations

2 Documents

2.1 Applicable Documents

- A - 1: W7714-040875/001/SV, Contract for the Technology Demonstration of the Joint Network Defence and Management System (JNDMS), PWGSC.
- A - 2: DN0648, Project Management Plan for the Technology Demonstration of JNDMS Project, MDA.
- A - 3: DN0647, Configuration Management Plan for the Technology Demonstration of JNDMS Project, MDA.

2.2 Reference Documents

- R - 1: DN0665, System Requirements Specification for the Technology Demonstration of JNDMS Project, MDA.
- R - 2: DN0678, Design Document for the Technology Demonstration of JNDMS Project, MDA.
- R - 3: Using a VMWare Network Infrastructure to Collect Traffic Traces for Intrusion Detection and Evaluation, Communications Research Centre.

3 Testing Overview

3.1 System Testing Objectives

The overall objectives of JNDMS testing are as follows:

- To validate, through testing, that the JNDMS complies with the system requirements. Test descriptions will be documented and will be traceable to stated system requirements and any System Change Requests (SCR) approved for implementation.
- To document issues that arise during system testing in sufficient detail to carry out complete and timely resolution of the issue.

The delivery of the JNDMS will constitute one of the events contributing to the completion of each development cycle during Phase 2.

3.2 JNDMS Testing

JNDMS testing will be accomplished in a phased and iterative fashion (three cycles). This incremental process will allow for controlled testing of the system requirements. Incremental testing allows DRDC and MDA to verify requirements and disposition any discrepancies prior to the delivery of the system. The major benefit of this process is a system that is delivered on time with customer knowledge of functionality and discrepancies. This process also saves time - by verifying requirements incrementally, both DRDC and MDA understand the performance level of each of the Software Configuration Items (SWCI) and Hardware Configuration Items (HWCI) at the end of each development cycle.

JNDMS testing begins with the definition of testable requirements and concludes with the successful demonstration of requirements during the Phase 2 development cycles. Various types of testing will be used to verify and validate that the JNDMS achieves the system requirements. The testing methods are:

1. Inspection
2. Demonstration
3. Analysis
4. Inference

In some instances, requirements span more than one cycle. Where possible, portions of these spanning requirements are tested in individual cycles. The requirement is not considered satisfied until the complete requirement, as stated, has been verified. Early (Cycle 1 and 2) testing of portions of the spanning requirement helps reduce the overall risk of fulfilling it and can be considered a partial completion of the requirement.

3.3 JNDMS Testing Environment

The testing environment for JNDMS is an extension of the development environment, as discussed in the JNDMS Design Document [R-2]. Figure 1 shows the development environment as it will be configured during Cycle 1.

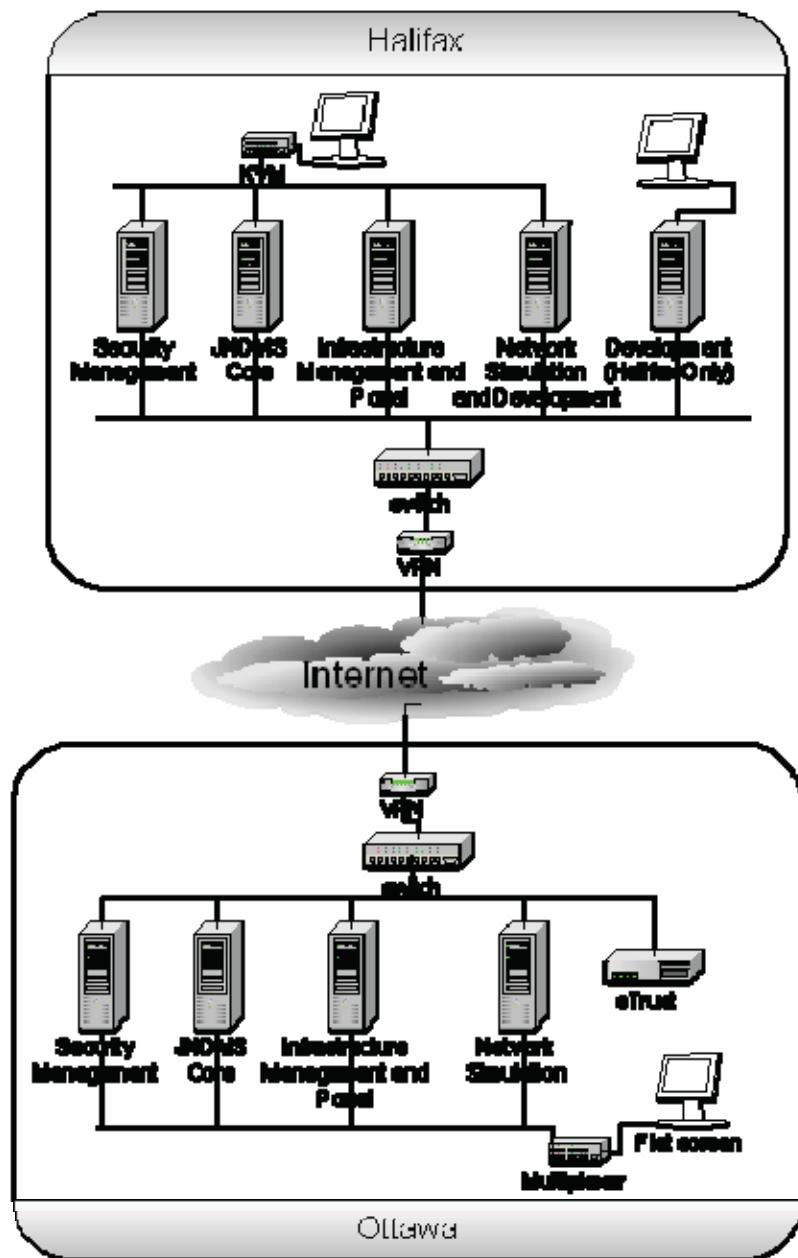


Figure 1: JNDMS Development Environment

The description of these workstations and their role within the environment is shown in Table 1.

Table 1: Cycle 1 Workstation Configuration

ID	Environment	Qty.	Development Role	Key Applications	Guest Env. (ID)	OS
1	Security	2	Host workstation for security management	VMWare Server	1. ISM (7)	Redhat ES 4
2	Core	2	Database, Core Services	VMWare Server Oracle Jboss ESRI ArcGIS	1. Aion (9)	Redhat ES 4
3	EIM / Portal	2	Host workstation for Infrastructure Management and Portal	VMWare Server	1. Unitcenter (11) 2. Portal (12)	Fedora Core 4
4	Network Simulation	1	Host workstation for network simulation and Linux development support	VMWare Server	1. Development A (13) 2. Host A (14) 3. Host B (15) 4. Host C (16) 5. Host D (17)	Fedora Core 4
5	Network Simulation and Development Support	1	Development support and host workstation for network simulation and Linux development support	VMWare Server Subversion	1. Development A (13) 2. Host A (14) 3. Host B (15) 4. Host C (16) 5. Host D (17)	Fedora Core 4
6	Development	1	Windows Development Environment	Windows Development	None	Windows XP Pro

Table 2 provides a brief description of the virtual environments that are to be part of the development environment.

Table 2: Configuration of Virtual Environments

ID	Environment	Qty.	Development Role	Key Applications	OS
7	ISM	2	Core of security management	ISM Nessus Server	Redhat ES 4
8	Data Warehouse	0	Data Warehouse, including the GIS data	Oracle ESRI ArcGIS Server	Redhat ES 4
9	Aion	2	Development and configuration of Aion	Oracle Aion	Redhat ES 4
10	Core	0	Core components of the JNDMS	JBoss Aion	Redhat ES 4
11	Unicenter	2	Platform for CA tools	Unicenter NSM Unicenter Asset Management eTrust Vulnerability Manager	Windows Server 2003
12	Portal	0	Responsible for presentation layer	Cleverpath Portal	Windows XP
13	Development A	2	Base of Linux development environment	Test environments	Fedora
14	Host A	2	Sample host	Asset, eTrust agents	Windows XP
15	Host B	2	Sample host	No agents	Windows XP
16	Host C	2	Sample host	Asset, eTrust agents	Fedora
17	Host D	2	Sample host	No agents	Fedora

The workstation environment for Network Simulation and Development Support (environment ID #5) will be used to support the running of unit tests and allow a central location for building the system and running tests.

The test environment will support the Cycle 1 testing by providing a basic setup that can be used to generate events in a controlled manner. The use of virtual machines allows us to easily enable or disable the environments to simulate the loss of a server, and the use of both labs allows us to simulate two Service Delivery Areas. Sample positions will be assigned to the various environments to show the Geological distribution of the two sites.

3.4 Test Data

The Cycle 1 development will concentrate on the core of the integration, and the testing will reflect this focus. The majority of the test data for Cycle 1 will make use of the JNDMS core services interfaces. This is a SOAP (Simple Object Access Protocol) Web Services interface that defines the primary inputs and outputs for the core decision support system.

The primary source of test data for Cycle 1 will result from running the input systems and capturing the XML that is communicated to the JNDMS core services. These XML packets represent all of the information that JNDMS decision support knows about the networks and operations and, therefore, represents the entire picture at a high level. These XML packets will be stored as file and can then be hand edited to inject events that are not easily reproduced in our test environment. This combination of captured data and crafted events will provide the primary method of generating the test data during Cycle 1.

The data captured from the development environment will be sufficient to prove many of the system integration and user interface issues to be examined during the first cycle, however, as the system grows the realism and complexity of the test data must also grow. The next level of test data will be to generate more complex network topologies. During the first cycle, a topology generator called Brite (<http://www.cs.bu.edu/brite/>) will be used to generate events. Brite creates a text output file that represents the generated topology, including bandwidth descriptions. As part of the test framework a parser will be written to generate JNDMS XML events from the Brite output files. This will allow some scenarios to be tested that rely on more complex network structures. During the first cycle, we will rely on a modified version of the data captured from the development environment to simulate events.

The goal of using Brite is to create several simulated Service Delivery Areas (SDA) with distributed servers and services that can be used to build more complex scenarios in the future development cycles.

One possible source of test inputs could result from any demonstrations or experiments run on a network outside of the test environment. It is unlikely that Cycle 1 will provide this opportunity, however, any experiments or demonstrations will result in a captured set of JNDMS XML files, which can then later be replayed or edited to provide additional sources of inputs.

Another source of data that can be leveraged is the use of data captured from the Packet Capture Library (PCAP). There are possible third party datasets of this type of data that include signatures of attacks. The integration of this type of data would be done not at the XML layer for the JNDMS core services, but integrated into the security and infrastructure management tools. The integration of these data sources will be examined during Cycle 1, however, no test data will be generated or used from PCAP data.

4 Testing Activities and Events

The following testing related activities and events will be governed by this Test Design Document:

- Unit Testing
- Integration/Pre Trials Testing
- JNDMS Experiments
- JNDMS Ad-hoc Demonstrations
- JNDMS Trials
- JNDMS Formal Demonstrations

4.1 Unit Testing

Unit testing will be performed on all individual components of the JNDMS. Unit testing is the responsibility of the JNDMS engineer assigned the task of completing the component under test.

A unit test description will be prepared for all unit tests. The unit test descriptions are to be written so that each test can determine if it passes or fails; this will allow for a large number of test cases to run. The unit test description will be prepared and executed by the JNDMS engineer responsible for the unit under test. The unit test code or documents are to be maintained in the configuration management (CM) repository, however, they will not be placed under formal data management procedures.

Candidate unit tests will be configured to run as part of a regression style test set. These unit tests must each provide the success or failure of the test without user intervention.

4.2 Integration

Integration testing will be performed towards the end of each development cycle in Phase 2. Integration testing is the responsibility of the JNDMS Integration and Test (I&T) engineer. Quality Assurance (QA) witnessing will be required during the final 5 days of integration testing.

Integration Testing is conducted to provide the following:

- Verification that the individual modules perform as expected when integrated into a larger system
- Verification that the JNDMS is ready for formal trials
- Validation of completeness and adequacy of the test cases and procedures to be used for trials

4.3 Experiments

Experiments consist of measuring the capability, performance and quality attributes of specified JNDMS features. Experiments will have both a performance testing and research/exploratory element to them. Experiments may occur at any time during the Phase 2 development cycles. MDA has planned for a minimum of 10 person-weeks per development cycle to conduct and support JNDMS experiments. Experiments primarily involve the MDA JNDMS project team members and potentially the DRDC JNDMS PM. MDA will plan, setup, conduct and report on JNDMS experiments. Experiments may be proposed by both the DRDC and MDA project teams but are subject to the DRDC JNDMS PM approval. Additionally, during Phase 2, MDA will support the use of the JNDMS in Defence experiments, which may be combined with trials and demonstrations (e.g. Coalition Warrior Interoperability Demonstration [CWID]), and may involve national and international stakeholders, such as The Technology Collaboration Program (TTCP) and the United States (US) Advanced Concept Technology Demonstration (ACTD). Support entails preparing, deploying, and operating the JNDMS for the exercise, as well as reporting on the exercise.

Experiments differ from internal testing in that:

- Outcomes are less certain
- There is a wide range of possible inputs
- May have a broader research interest

JNDMS experiments do not constitute formal acceptance testing; however, they will be conducted in a manner similar to JNDMS trials with the exception that formal QA witnessing will not be required for experiments.

4.4 JNDMS Ad-hoc Demonstrations

DRDC may schedule ad-hoc demonstrations at any time during the Phase 2 development cycles. MDA has planned for 5 person-days per development cycle to support these ad-hoc demonstrations. MDA will produce demonstration material in support of ad-hoc demonstrations and other communications activities for the DRDC JNDMS PM.

4.5 JNDMS Trials

The JNDMS trials will constitute the formal system evaluation by the DRDC JNDMS PM and the operational community. The intent of the trials is to evaluate the system and the quality of the resultant network situational awareness (SA) and direct (or re-direct) the project accordingly. Each trial shall represent a key evaluation exercise within the JNDMS project. Trials will occur at the end of each development cycle and will be designed to evaluate the overall behaviour and performance of the system. They will be based on scenarios, which reflect the real operational environment of the system. The DRDC JNDMS PM, MDA and user community representatives will be involved. MDA will be responsible for the planning, setup, conduct and reporting on JNDMS trials, as well as supporting the evaluation of JNDMS by the DRDC JNDMS PM.

It is intended that Cycle 1 and Cycle 2 trials occur at the MDA Halifax facilities. Cycle 3 trials are intended to take place on sections of the Department of National Defence (DND) experimental or operational networks. For this trial, significant effort will be spent deploying the JNDMS and integrating scenarios with the environment. MDA will work with the DRDC JNDMS PM, DND Information Management (IM), Information Technology (IT) and security organizations, as well as the operational community to deploy temporarily the JNDMS.

4.6 JNDMS Formal Demonstrations

Demonstrations are vital for maintaining operational client support and for generating national and international interest in the JNDMS project. Compared to experiments and trials, the demonstrations are not really about testing the JNDMS; rather, they are focused on demonstrating system capabilities to JNDMS stakeholders.

The JNDMS formal demonstrations will take place at the end of each development cycle in Phase 2 after the completion of trials. A period of up to two weeks has been reserved for demonstration support at the end of each development cycle.

All demonstrations shall be conducted at Crown's facilities. The final system demonstration could take place on a portion of the DND IT infrastructure. MDA will provide technical personnel cleared to SECRET level in support of this final demonstration.

5 Testing Methodology and Execution

This section discusses the testing methodology and test execution for JNDMS, including unit testing, integration testing, experiments, trials and demonstrations.

5.1 Unit Testing

Unit testing is the responsibility of the JNDMS engineer responsible for the unit/module under test. Unit testing will be primarily “white box” testing and may include some or all of the following activities:

- Code Reviews / Code Walkthrough
- Functionality based testing may include:
 - Path coverage
 - Boundary condition test cases
 - Error testing

The unit test descriptions, how to validate results and the test scripts and code will be kept up-to-date with the associated unit or module. This is the responsibility of the JNDMS engineer responsible for the unit or module being tested. The JNDMS Project Engineer (PE) will identify, with the developers, candidate unit tests that can be used to quickly verify the state of a build.

5.2 Integration Testing

Integration testing is the responsibility of the JNDMS I&T engineer. Integration testing will be primarily “black box” testing; however, it will include white and grey box testing where considered necessary.

Integration testing will be primarily requirements based testing. Integration testing will include all test cases intended for the development cycle trials. The final period of integration testing will include a QA witnessed dry run of the trials test cases.

Integration testing will also include some functionality based testing where multiple units are required to demonstrate specific functionality.

Integration testing will also include database table examination where considered necessary.

During integration testing test issues will be raised and passed to the PE, System Engineer (SE) and JNDMS engineer responsible for the module/ application against

which the issue has been raised. The PE, SE and responsible engineer will analyze and prioritize the issues for rectification. Issues that could have an adverse effect on the cycle trials and or demonstrations will be given the highest priority and will need to be rectified and retested prior to the commencement of the cycle trials. Other issues that can be addressed and retested prior to the trials period for the cycle will also be addressed. After the system is placed in integration testing, no further new development is to be conducted. All development effort during this period will be dedicated to issue resolution.

5.3 Experiments

Experiments will be conducted in accordance with an experiment report describing the nature of the experiment, the objectives and the results to be prepared for every experiment. The experiment report will properly plan each experiment, allow for sufficient time to involve DRDC scientist when applicable, and capture the results. The experiment report will be prepared in two deliveries. Delivery 1 will be a draft experiment report delivered to DRDC no later than 10 working days before each experiment and will include the following:

- Experiment's objectives
- Hypothesis
- Experiment items (software, component, etc.)
- Features to be tested
- Features not to be tested
- Scenarios and test cases
- Intended approach
- Intended set-up and facilities
- Metrics
- Tasks and responsibilities
- Needs (access to data sources, clearance, etc.)
- Required staffing and training
- Intended schedule and location

Delivery 2 will be the final experiment report delivered to DRDC no later than 10 working days after each experiment and will include the following:

- Experiment's objectives
- Hypothesis
- Experiment items (software, component, etc.)
- Features tested
- Features not tested
- Scenarios and test cases
- Actual approach

- Actual set-up and facilities
- Metrics
- Tasks and responsibilities
- Needs (access to data sources, clearance, etc.)
- Staffing and training
- Actual schedule and location;
- Data captured during the experiment (if applicable)
- Results and interpretation
- Minutes of discussions (if applicable)

5.4 JNDMS Trials

JNDMS trials will be “black box” requirements based testing. All test cases will be based on the JNDMS scenarios contained in section 7 of this Test Design Document. The Cycle 2 and Cycle 3 trials will include regression testing for requirements considered delivered in previous cycles.

A trial report describing the nature of the trial, the objectives, the activities and the results will be prepared for each trial. The trial report will be prepared in two deliveries. Delivery 1 will be a draft trial report delivered to DRDC no later than 15 working days before each experiment and will include the following:

- Test items (software, component, etc.)
- Features to be tested
- Features not to be tested
- Scenarios and test cases
- Intended approach
- Required participants
- Tasks and responsibilities
- Intended set-up and facilities
- Planned metrics (including evaluation criteria)
- Needs (access to data sources, clearance, etc.)
- Intended staffing and training
- Planned schedule and location

Delivery 2 will be the final experiment report delivered to DRDC no later than 10 working days after the trials and will include the following:

- Test items (software, component, etc.)
- Features tested
- Features not tested
- Scenarios and test cases

- Approach followed
- Participants present
- Tasks and responsibilities
- Set-up and facilities
- Metrics (including evaluation criteria)
- Needs (access to data sources, clearance, etc.)
- Staffing and training
- Schedule and location
- Data captured during the trial (if applicable)
- Results
- Minutes of discussions and comments during the trial

5.5 JNDMS Demonstrations

Demonstrations, both ad-hoc and formal, are not specifically about testing the JNDMS; rather, they are focused on demonstrating system capabilities to JNDMS stakeholders. As the intent of demonstrations is not testing they will be conducted primarily using black box methodologies. In general it is the intent that demonstrations be fully “scripted” and follow specific scenarios as detailed in section 7.

6 Resources, Schedule and Deliverables

The test environment will be representative of the DND IT infrastructure environment as much as possible. The constraints and requirements pertinent to this environment will be described in the System Requirements Specification document [R-1] and will be refined during Phase 1.

6.1 Unit Testing

6.1.1 Resources

Table 3 lists the personnel resources required for unit testing.

Personnel	Responsibilities
JNDMS Engineer Responsible for the Unit	<ul style="list-style-type: none">• Producing Unit Test Cases• Providing Unit Test Drivers/Stubs• Conducting Unit Testing• Documenting Unit Test Results• Conducting Code Reviews• Maintaining Unit Test Description with code base (in CM Tool)
PE	<ul style="list-style-type: none">• Verifying Unit Testing Completed for all Units/Modules• Identify automated unit tests for validating new system builds (regression style tests)

Table 3: Unit Testing Personnel

The following resources are necessary for unit testing:

- The Unit Under Test
- Unit Test Cases
- Test Drivers and Stubs (when required)

6.1.2 Schedule

Unit tests are to be completed as soon as possible after the unit/module under test is ready for testing. The JNDMS engineer responsible for the unit is to ensure the PE is advised of the scheduled time for all unit testing.

6.1.3 Deliverables

The following internal deliverables are required on completion of unit testing:

- Unit Test Cases
- Unit Test Results
- Updated Software Development Folders

6.2 Integration Testing

6.2.1 Resources

Table 4 lists the personnel resources required for integration testing.

Table 4: Integration Testing Personnel

Personnel	Responsibilities
JNDMS Development Engineers	<ul style="list-style-type: none">• Complete unit testing• Check unit tested modules into JIRA• Update issues to indicate that they have been addressed• Provide build/install Instructions• Address integration test issues assigned
CMC	<ul style="list-style-type: none">• Create tags• Extract tags

Personnel	Responsibilities
I&T	<ul style="list-style-type: none"> • Create integration test cases • Build/install system to be tested • Ensure all regression tests pass • Conduct integration testing • Identify problems and issues • Raise test issues
PE	<ul style="list-style-type: none"> • Assign test engineer to assist in integration testing (if required) • Prioritize/assign test issues for rectification
QA	<ul style="list-style-type: none"> • Provide formal QA witnessing for final period of integration testing
Testing Engineer (Responsibilities may be performed by I&T)	<ul style="list-style-type: none"> • Under direction from I&T, run test cases • Assist in identifying test issues
NRNS Support	<ul style="list-style-type: none"> • When required, provide NRNS support for integration testing
Computer Associates (CA) Support	<ul style="list-style-type: none"> • When required, provide CA support for integration testing

The following resources are required for integration testing:

- JNDMS software (commercial off-the-shelf [COTS] and custom) to be integrated and tested
- Integration test cases and scenarios
- The following JNDMS hardware:
 - *Hardware resources to be identified when hardware is acquired for JNDMS*

6.2.2 Schedule

Integration testing will be scheduled towards the end of each development cycle to be completed prior to the conduct of trials. Integration testing will commence when all new development scheduled for the development cycle has been completed. The CM Coordinator (CMC) will produce a testing baseline of the JNDMS software and hardware configuration at the commencement of integration testing. No new development will be conducted during integration testing, and all development effort will be directed towards

issue resolution. It is intended that integration testing will take up to three weeks to complete.

The CMC will produce an updated testing baseline of the JNDMS at the beginning of the final week. This updated baseline will be used as the JNDMS system for QA witnessing prior to trials.

The final week of integration testing will be a QA witnessed dry run of the JNDMS trials for the development cycle.

6.2.3 Deliverables

The following internal deliverables are required on completion of unit testing:

- Validated development cycle trials test cases
- Baseline JNDMS for development cycle trials
- Integration test results
- Updated Software Development Folders

6.3 Experiments

6.3.1 Resources

Table 5 lists the personnel resources required for experiments.

Table 5: Experiments Personnel

Personnel	Responsibilities
Experiment Originator	<ul style="list-style-type: none">• Provide experiment's objectives• Provide experiment's hypothesis• Determine experiment items (software, component, etc.)
CMC	<ul style="list-style-type: none">• Create experiment tag• Extract experiment tag

Personnel	Responsibilities
I&T	<ul style="list-style-type: none"> • Create draft experiment report • Build/install system for experiment • Ensure regression tests pass • Act as test conductor for experiments • Document experiment results • Raise Test issues • Complete Final Experiment Report
PE	<ul style="list-style-type: none"> • Assign test engineer to assist as JNDMS operator for experiment (if required)
Test Engineer (Responsibilities may be performed by I&T)	<ul style="list-style-type: none"> • Conduct experiment(s)
NRNS Support	<ul style="list-style-type: none"> • When required, provide NRNS support for experiments • When required, provide JNDMS System Administration support for experiments conducted at Crown facilities
CA Support	<ul style="list-style-type: none"> • When required, provide CA support for experiments
DRDC PM	<ul style="list-style-type: none"> • Determine DRDC desired level of involvement in the experiment and assign DRDC resources as necessary • Provide DRDC experiment witness(es) as necessary

The following resources are required for experiments:

- JNDMS software (COTS and custom) to be identified on an experiment by experiment basis
- Draft experiment report
- JNDMS hardware, to be identified on an experiment by experiment basis

6.3.2 Schedule

Experiments will be scheduled when required during each development cycle. It is intended that all experiments to be conducted during a development cycle be completed a minimum of 5 working days prior to commencement the cycle integration testing.

It is intended to schedule three distinctive one-week periods during each development cycle for the conduct of experiments. Where possible, experiments will be conducted in a sequential manner during one of the one-week periods.

6.3.3 Deliverables

The following deliverables are required for experiments:

- Draft Experiment Report, not later than 10 days prior to conducting the experiment
- Final Experiment Report, not later than 10 days after conducting the experiment

6.4 Trials

6.4.1 Resources

Table 6 lists the personnel resources required for trials.

Table 6: Trials Personnel

Personnel	Responsibilities
JNDMS Development Engineers	<ul style="list-style-type: none">• Address integration test issues assigned• Complete unit testing• Check unit tested modules into JIRA• Update issues to indicate that they have been addressed• Update build/install instructions (if required)
CMC	<ul style="list-style-type: none">• Create tags• Extract tags

Personnel	Responsibilities
I&T	<ul style="list-style-type: none"> • Create draft trials report • Build/install system to be tested • Ensure regression tests pass • Prepare Trials Readiness Review (TRR) brief • Conduct TRR • Act as trials conductor for trials • Note problems and issues • Raise test issues • Complete final trials report
PE/PM	<ul style="list-style-type: none"> • Assign test engineer to assist as JNDMS operator • Determine MDA pass/fail assessment for each test case
QA	<ul style="list-style-type: none"> • Provide formal QA witnessing for trials
Test Operator	<ul style="list-style-type: none"> • Under direction from I&T, run test cases • Note test issues
NRNS Support	<ul style="list-style-type: none"> • When required, provide NRNS support for trials • When required, provide JNDMS System Administration support for trials conducted at Crown facilities
CA Support	<ul style="list-style-type: none"> • When required, provide CA support for trials
DRDC PM/Test Witness	<ul style="list-style-type: none"> • Determine DRDC pass/fail assessment for each test case • Provide DRDC level of acceptance for JNDMS

The following resources are required for trials:

- JNDMS software (COTS and custom) to be tested
- Draft trials report
- The following JNDMS hardware:

- *Hardware resources to be identified when hardware is acquired for JNDMS*

6.4.2 Schedule

Trials will be scheduled towards the end of each development cycle. A period of up to 5 working days will be scheduled for each trial.

For JNDMS trials, a period of up to 1 day will be allocated to the installation, configuration and verification of the JNDMS trials system. On completion of verifying the JNDMS for trials, a TRR will be conducted. This TRR will take approximately 0.5 days. It is anticipated that 2 to 3 days will be required to perform the actual trials. On completion of executing the trials, it is intended that a post trials wrap-up of approximately 0.5 days will be conducted.

6.4.3 Deliverables

The following deliverables are required for trials:

- Draft Trial Report, not later than 15 days prior to conducting the trial
- Final Trial Report, not later than 10 days after conducting the trial
- Updated Requirements Traceability Matrix

6.5 Demonstrations

6.5.1 Resources

Table 7 lists the personnel resources required for formal demonstrations. Depending on the nature of ad-hoc demonstrations, a subset of these personnel may be required.

Table 7: Formal Demonstrations Personnel

Personnel	Responsibilities
CMC	<ul style="list-style-type: none">• Create external tags• Extract external tags• Collect and provide demonstration materials, as necessary
I&T	<ul style="list-style-type: none">• Create demonstration procedure

Personnel	Responsibilities
	<ul style="list-style-type: none"> • Build/install system to be tested • Ensure regression tests pass • Act as demonstration conductor for trials • Note any problems and issues
PE/PM	<ul style="list-style-type: none"> • Assign test engineer to assist as JNDMS operator • Witness formal demonstrations
Testing Engineer (Responsibilities may be performed by I&T)	<ul style="list-style-type: none"> • Under direction from I&T, run demonstration procedures • Note any problems and issues
NRNS Support	<ul style="list-style-type: none"> • When required, provide NRNS support for demonstrations • Provide JNDMS System Administration support for demonstrations at Crown facilities
CA Support	<ul style="list-style-type: none"> • When required, provide CA support for demonstrations
DRDC PM	<ul style="list-style-type: none"> • Determine demonstration location • Determine and provide demonstration objectives • Provide overall direction for demonstrations

The following resources are required for Demonstrations:

- JNDMS software (COTS and custom) to be demonstrated
- Demonstration materials, including the necessary hardware to be identified on a demonstration by demonstration basis
- Demonstration procedures

6.5.2 Schedule

Formal demonstrations will be scheduled at the end of each development cycle. A period of between one and three weeks is scheduled for each formal demonstration.

Ad-hoc demonstrations will be scheduled when required during each development cycle. It is intended that all ad-hoc demonstrations to be conducted during a development cycle be completed a minimum of 5 working days prior to commencement of the cycle integration testing. Five person days per development cycle will be allocated to ad-hoc demonstrations.

6.5.3 Deliverables

The following deliverables are required for demonstrations:

- Demonstration materials
- Where the demonstration is in support of demonstrations (e.g. CWID) or involves national and international stakeholders, such as TTCP and US ACTD, a report on the exercise shall be prepared.

7 JNDMS Test Scenarios

JNDMS scenarios to be updated and completed during each development cycle to ensure functionality scheduled for each development cycle is fully covered.

These scenarios are used to evaluate the system, especially during Integration and Test activities. During the development cycles, test input data will be collected to support each of the scenarios. Cycle 1 will make use of captured and modified JNDMS XML input files (see section 3.4). These captured and modified input files will test as much of each scenario as possible with the functionality available during Cycle 1.

7.1 Scenario 1 - System Familiarization

Objective: To familiarize a Network Operations Center (NOC) operator with the JNDMS.

Use Case(s) Addressed:

- User Interactions

Background: The JNDMS has recently been installed at National Defence Headquarters' (NDHQ) NOC and a NOC operator responsible for monitoring the system has been informed that the NOC OIC wishes to be given a briefing the next morning on the capabilities of the system.

Scope: The operator has been informed to keep the scope of the briefing at a regional level.

Configuration and Preconditions:

- The system is to be configured to monitor local NDHQ networks in an initial delivery configuration.
- The networks are to be in a standard operating condition with no incidents occurring.
- The network activity is to be representative of a night watch – between 0200 and 0600 hrs.

Roles and Tasks:

User has access to all roles.

User has ability to perform all tasks.

Sequence of Activities:

1. User logs on to JNDMS as the JNDMS system administrator and is presented with the initial view.
2. User creates a user defined view by selecting the type of display and default parameters (location, zoom level, etc.).
3. User creates user-defined queries.
4. User stores user defined view and queries in user profile.
5. User logs off.
6. User re-logs on and is presented with the user-defined view.
7. User uses user-defined queries.
8. User makes use of Geospatial map overlay, logical network graphs, data tables and other data presentation schemes.
9. User makes use of the toolbar to display and filter the data.
10. User uses the Equipment view Query Table to query for operations depending on IT infrastructure assets (equipment, services, networks or circuits).
11. User views the visual correlation of network views as they evolve in time, using features such as "playback".
12. User performs "drill-down" "drill-up" and "drill-across", and contextual navigation capabilities to the details of the data repositories.
13. User creates new rules and changes existing rules.
14. User changes the thresholds for report generation, incident recognition and severity assessment.
15. User logs off.
16. User logs on as a Commander and is presented with the initial display.
17. Repeat steps 15 and 16 for the Vulnerability and Security Analysts and the Network Manager roles.

7.2 Scenario 2 - Headquarters Staff Checks Network Status

Objective: Provide SA of networks supporting an operation

Use Case(s) Addressed:

- Headquarters staff checks network status

Background: A Colonel watches the JNDMS tool for 30 seconds to confirm that the IT infrastructure for an operation is back to normal.

Scope: Regional or Deployed

Configuration and Preconditions:

Regional Scope:

- The system is to be configured to monitor local NDHQ networks in an initial delivery configuration.
- The networks are to be in a standard operating condition with no incidents occurring.

Deployed Scope

- The system is to be configured to monitor local NDHQ networks in an initial delivery configuration.
- The system is to be provided inputs from a simulated deployed operational network consisting of:
 - A Command and Control Application (Global Command and Control System [GCCS] or Athene)
 - A file server
 - Four workstations
- The networks are to be in a standard operating condition with no incidents occurring.

Roles and Tasks:

TBD

Sequence of Activities:

1. A Colonel in headquarters who is responsible for an operation decides to check the current status of the networks supporting the operation. The Colonel invokes the JNDMS tool. The expectation is that the user will invoke JNDMS to view the information that it is processing.

2. The JNDMS logon screen appears along with an icon indicating that a change in the network status has occurred. The JNDMS can be configured based on the user profile to take an action such as beep at the workstation or display an icon if a change happens. A change could be, for example, the occurrence of a security incident.
3. The Colonel types a user identifier and a password in the logon screen of JNDMS and presses the Enter key. This logs the user in and causes JNDMS to bring up its initial display as specified in the user profile. The user can specify what this initial view will be.
4. In this case, all of the network nodes and links are coloured green indicating that the network is operating within the rule limits configured by the System Administration staff, since the legend selection is "availability status". Selecting a security view would show colours that reflect rules configured by the security analysts. The Colonel sees that the entire network is operational.
5. The information presented by the JNDMS is dynamically updated every 10 seconds (approximation depending on bandwidth requirements and availability). Each map window updates its information independently by polling the JNDMS server. The Colonel watches the screen for 30 seconds, knowing that the lack of change implies that the network status is not changing. Each map window indicates that it is being refreshed as the polling steps complete so the user is confident that the tool is running as expected.
6. The Colonel, satisfied that the network is back to normal, clicks the Exit button to end this session. JNDMS does not log user actions, so no record is kept of this session.

7.3 Scenario 3 - Isolation of a Local Domain

Objective: Isolate a local domain on a Wide Area Network to investigate and correct an error condition.

Use Case(s) Addressed:

- Isolation of a Local Domain

Background: A security analyst responsible for a Metropolitan Area Network suspects that some malicious code has been placed on the network, and it is causing the loss of services on many hosts. Using JNDMS, the cause of the problem is revealed and the problem is resolved without disrupting users who were not affected by the problem.

Scope: National

Configuration and Preconditions:

- The system is to be configured to monitor a Regional area DWAN type of environment consisting of several domains connect via a Regional Router:
 - The NOC's primary Metropolitan network serving the local Metropolitan area
 - Domain A – a simulated secondary Metropolitan Area Network serving facilities in an adjoining Metropolitan Area and sharing the Regional Router connectivity to the National Network
 - Domain B – The simulated remainder of the National Network outside the Regional Router.
 - Domain C – A simulated specialized Local Area Network sharing the Regional Router connectivity to the National Network
- Simulated inputs are to be fed to the JNDMS from Domains A, B, C. The local JNDMS is to be monitoring the inputs on the NOC's primary Metropolitan network.

Roles and Tasks: TBD

Sequence of Activities:

1. Initially all domains that constitute this network are running without any incidents. Active network information gathering components are running in each domain (i.e. A, B, and C) and at the NOC. The data that the domains collect is pushed to their own JNDMS database and to the JNDMS database at the NOC. These components have been set up to probe for the existence of two services on every machine in their domain, namely: Login, and VirusScan. The components collect this data and send it on periodically, e.g. every 10 seconds.

2. At 1004 hrs, the System Administration person in "A" Domain runs a script that incorrectly removes the Login and VirusScan services from most of the machines in the domain. The System Administration person is not aware of this error and the fact that running the script caused a problem.
3. The System Administration person continues to work and notices that login is not possible on some machines. This is unexpected, and the System Administration person cannot login anywhere to check further or make corrections. The System Administration person telephones the "A" Domain Help Desk and causes an "A" Domain trouble ticket to be raised. The existence of a trouble ticket is a monitored item for the JNDMS, so the local JNDMS database and the JNDMS database at the NOC receive this data.
4. The System Administration person contacts the local Security Analyst who is using a machine that is always logged in and is not affected by the current problem. The Security Analyst is currently running JNDMS and has the "Security Events" view selected. The Security Analyst has received several alerts about unexpected changes on "A" Domain.
5. In the "Security Events" view, the host sites for which an alert has been raised are coloured red. The Security Analyst clicks on one red host site and sees an alert summary. It indicates that the Login and VirusScan services have not been running since 1005 hrs. The Security Analyst then adds the "services status" view with columns indicating which services are running. Login and VirusScan are not running on hosts where alerts were raised. The Security Analyst steps this view back and sees that these services were running correctly on all hosts at 1003 hrs.
6. The Security Analyst returns to the general monitoring view for alerts, and selects a view that displays all the domains and the primary network. This information indicates that the missing service problem is restricted to "A" Domain.
7. The Security Analyst then queries the Operations and Infrastructure dependencies database and determines that no operations are dependent on "A" Domain. It can be isolated without operational impact.
8. The Security Analyst telephones the NOC to report that the situation is suspicious, but apparently localized. This data is added to the "A" Domain trouble ticket. The Security Analyst recommends that "A" Domain be isolated.
9. The NOC uses JNDMS to confirm the Security Analyst's report and reaches the same conclusion. They then isolate the "A" Domain by stopping the connection between "A" Domain and the router. "A" Domain and NOC are now isolated, and the information held in their instances of JNDMS begins to diverge. At this point, NOC begins to review external sources, such as Computer Emergency Response Team (CERT), to determine if the observed symptoms correspond with any currently known exploits. No evidence of related problems is found.
10. Meanwhile, the System Administration person discovers the error in the script that caused this problem, and makes the necessary corrections. "A" Domain is now operating as expected. The Security Analyst monitors the local situation using the JNDMS services view locally to collect evidence that everything is working correctly. The System Administration person telephones NOC and recommends that "A" Domain be connected to the router.

11. NOC reconnects "A" Domain and monitors its behaviour closely for a short time. The trouble ticket is closed.

7.4 Scenario 4 - Physical Damage

Objective: To assess the impact of damaged equipment and formulate a course of action to minimize the effects on the operational network and local operations.

Use Case(s) Addressed:

- Physical Damage

Background: Physical damage at a specific location has an impact on many services and operations. The JNDMS ability to reveal these impacts quickly is important for mitigating the impact of physical damage during an emergency

Scope: Local

Configuration and Preconditions: TBD

Roles and Tasks: TBD

Sequence of Activities:

1. Water damage begins in a room that contains several pieces of equipment used by various networks and services. Initially, it is clear that all the equipment in this room will have to be shut down, but the order in which this will take place is not clear. The System Administration staff want to make this disruption as graceful as possible.
2. The System Administrator uses the JNDMS central database to find out which equipment pieces are in the damaged room. The JNDMS supports queries that return the equipment located at specific locations. The information retrieved includes:
 - . What network each piece of equipment runs on
 - What services each piece of equipment supports
 - . The point of contact for each piece of equipment
3. Based on the services that will be disrupted, the System Administration person begins contacting the "point of contact" staff for the most critical services first. With their involvement, a plan is put into effect for mitigating the problems.
4. The JNDMS supports queries that return the operations and services depending on specific networks and pieces of equipment. This type of querying is crucial for mitigating the impact of physical damage. The operations that will be affected by these disruptions are notified by the System Administration staff involved in mitigating the problems. Given this warning, steps are taken within each operation to adjust its activities until the services are restored.
5. The water damage continues and all the equipment in the room is lost.
6. As a short-term solution, each damaged piece of equipment is replaced by a backup item. This restores all services, but in a degraded mode, since the network is not backed up now.

7. The original room and its equipment are restored. Services are put into full operation again. Operations are warned and make adjustments to minimize the impact of these switchovers to full service.

7.5 Scenario 5 - Response Based on Severity of Incidents

Objective: To prioritize response to multiple incidents based on the severity of the individual incidents

Use Case(s) Addressed:

- Response Based on Severity of Incidents

Background: The network shown in Figure 2 extends to four locations:

1. Router A is in DND Headquarters in Ottawa
2. Router B is in Montreal
3. Router C is on a deployed ship
4. NOC is in Ottawa

A security incident affects all the workstations on the network. The Security Analyst is able to decide which workstations to correct first using the severity calculation provided by JNDMS.

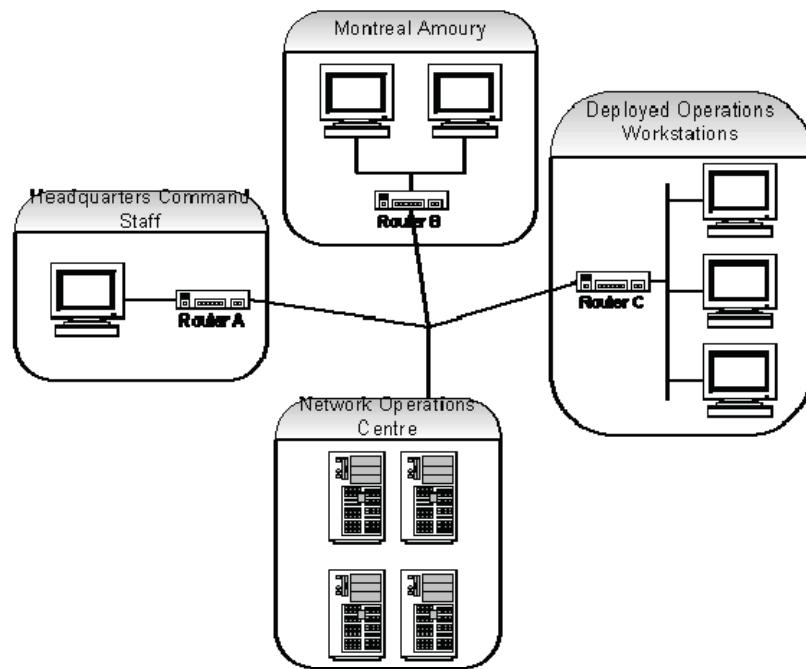


Figure 2: Network with Four Asset Locations

Scope: National

Configuration and Preconditions: TBD

Roles and Tasks: TBD

Sequence of Activities:

1. Six workstations at three sites, DND Headquarters in Ottawa, the Montreal Armoury, and HMCS Iroquois, generate identical alerts indicating that they are compromised by a Trojan program. The Trojan program is transmitting data from each workstation. The traffic created by this transmission has a signature pattern that JNDMS data analyzer components have detected on the local sub-network. The detection of this traffic pattern raised alerts at the NOC.
2. A Security Analyst at the NOC is looking at the JNDMS incident severity view. This view shows the locations of sites on a geographic background. The icon for DND Headquarters (i.e. Router A and its workstation) is red and shows a severity value of 17. The icon for HMCS Iroquois (i.e., Router C and its workstations) is red and shows a severity value of 18. The icon for the Montreal Armoury (i.e., Router B and its workstations) is yellow and shows a severity value of 11.
3. The Security Analyst clicks on the red icon for HMCS Iroquois (i.e. Router C), since this icon shows the highest severity value. This click brings into view a table of alert details, listing all the alerts raised at this site:

Timestamp	IP Address	Description	Severity
2003 Sep 03 14:52:28	150.24.11.1	Security-Trojan-Sub7	18
2003 Sep 03 14:52:33	150.24.11.2	Security-Trojan-Sub7	18
2003 Sep 03 14:52:38	150.24.11.3	Security-Trojan-Sub7	18

4. The Security Analyst clicks on one of the lines in this table to see the details about the severity calculation. In this case, all the alerts are the same, so clicking on any line brings up the following table:

Severity Parameter Name	Value	Descriptive Details
Location	3	HMCS Iroquois
Type of Incident	2	Security-Trojan-Sub7
Asset Type	1	Workstation
User Category	2	Operations Staff
Operations	3	Op Apollo
Network	1	DWAN
System/Application	0	N/A
Number of Alerts on same network	2	6

Severity Parameter Name	Value	Descriptive Details
Number of Alerts of same type	2	6
Number of Alerts at same location	2	3
Composite Severity	18	Section 8:

5. The Security Analyst clicks on the red icon for DND Headquarters (i.e., Router A), since this icon shows the next highest severity value. This click brings into view a table of alert details, listing all the alerts raised at this site:

Timestamp	IP Address	Description	Severity
2003 Sep 03 14:50:28	150.24.12.1	Security-Trojan-Sub7	17

6. The Security Analyst clicks on the line in this table to see the details about the severity calculation:

Severity Parameter Name	Value	Descriptive Details
Section 9: Location	3	HQ
Type of Incident	2	Security-Trojan-Sub7
Asset Type	1	Workstation
User Category	3	Command Staff
Operations	3	Op Apollo
Network	1	DWAN
System/Application	0	N/A
Number of Alerts on Same Network	2	6
Number of Alerts of Same Type	2	6
Number of Alerts at Same Location	0	1
Composite Severity	17	

7. The Security Analyst observes that the assets that have been compromised at DND Headquarters and at HMCS Iroquois are all associated with the same operation, OP Apollo. It appears that the network is being used to compromise this operation. The Security Analyst contacts the System Administration staff at HMCS Iroquois first since this is where the incident is having the most significant impact. The Security

Analyst provides the information needed to start the procedure for correcting this problem at HMCS Iroquois.

8. When the Security Analyst is available to address the next problem, the Security Analyst then telephones the System Administration staff at DND Headquarters and provides the information needed to start the procedure for correcting the problem there.
9. When the Security Analyst is available to address the next problem, the Security Analyst clicks on the icon for the Montreal Armoury since this icon shows the next highest severity value. This click brings into view a table of alert details, listing all the alerts raised at this site:

Timestamp	IP Address	Description	Severity
2003 Sep 03 14:55:15	150.24.10.1	Security-Trojan-Sub7	11
2003 Sep 03 14:55:18	150.24.10.2	Security-Trojan-Sub7	11

10. The Security Analyst clicks on one of the lines in this table to see the details about the severity calculation. In this case all the alerts are the same, so clicking on any line brings up this table:

Severity Parameter Name	Value	Descriptive Details
Location	1	Montreal Armoury
Type of Incident	2	Security-Trojan-Sub7
Asset Type	1	Workstation
User Category	1	Reserve Staff
Operations	0	N/A
Network	1	DWAN
System/Application	0	N/A
Number of Alerts on Same Network	2	6
Number of Alerts of Same Type	2	6
Number of Alerts at same location	1	2
Composite Severity	11	

11. The Security Analyst emails the System Administration staff at the Montreal Armoury to begin the procedure for correcting the problem there.

7.6 Scenario 6 - Working with a Coalition Partner

Objective: To use JNDMS data in collaboration with an ally.

Use Case(s) Addressed:

- Working with a Coalition Partner

Background: In response to a terrorist threat to the east coast of North America, Canada and the US have joined forces for the surveillance of the east coast. Computer networks belonging to both Canada and the US are critical assets for this operation. These networks are to be managed, monitored, and defended by the coalition team located in both countries. The JNDMS is interoperable with multinational tools to provide network operational status. The JNDMS provides network defence SA information for the Canadian portion of the networks used in this operation.

Scope: International

Configuration and Preconditions: TBD

Roles and Tasks: TBD

Sequence of Activities:

1. A JNDMS station located at the central NOC is connected to a multinational network. Information collected by the JNDMS is filtered through a guard and securely shared with allies. All nations share an “agreed upon” set of network defence SA information. The Common Operating Picture (COP) is designed to handle caveat separation so that individual nations can choose with whom they wish to share information.
2. For this operation, Canada and the US (having dealt with the appropriate foreign disclosure agreements) have agreed to share a more complete set of network defence SA information but only for the underlying network assets supporting the operation. The JNDMS is configured to filter information related to the Canadian networks supporting the operation and to push this information to coalition partners. Equivalent information from the US networks is fed to the JNDMS so that the Canadian Computer Network Defence (C-CND) team can view the status of the entire CA-US network.
3. A security event occurs on the US network. A web server has been compromised and is being used to covertly steal information using a variant of “HTTP Tunnel” through port 80.
4. A Canadian intrusion analyst is checking the status of the Canadian networks using their JNDMS console. The analyst sees a map of the Canadian networks, as well as a high level view of US networks. The analyst notices a red flashing dot at one of the network nodes located on a US base. In this case, the red dot signifies that a severe event has occurred at that location.

5. The analyst clicks on the red flashing dot to see details of the event. A screen pops up providing the event summary. In this case, the network event is security-related and involves a web server. Meanwhile, US analysts, alerted by their Intrusion Detection Systems (IDS), are investigating this event.
6. One Canadian analyst clicks on the “security alerts” option of the JNDMS console and is able to read details of the nature of the security event. The analyst then clicks on the “applications” option and sees that a Canadian web-based Command and Control (C2) tool depends on the compromised US server. The confidentiality and integrity of the C2 information may have been compromised.
7. The analyst selects the “defensive posture” view, highlighting all the security features of the web server. Immediately, the analyst finds out that the C2 tool was designed with built-in security features. All files related to the C2 tool are encrypted. Also, the analyst notices that the attacker cannot access Canadian hosts from the compromised web server.
8. Rather than immediately isolate the web server, which would disrupt the operation, the CND team takes extra time to remove the malicious code and secure the web server such that the attacker can no long steal information.

7.7 Scenario 7 - Maintenance Impacts Users

Objective: To use JNDMS data to minimize the impact of maintenance activities on the operational community.

Use Case(s) Addressed:

- Maintenance Impacts Users

Background: Bell Nexxia informs the NOC that a major upgrade is required on all ALCATEL multiplexing equipment over the entire Bell Nexxia infrastructure. This implies that major public and private clients of Bell, including banks, police, and governments will be affected. The proposed date for this maintenance is 30 days in the future.

Scope: Regional

Configuration and Preconditions: TBD

Roles and Tasks: TBD

Sequence of Activities:

1. A request is received by the NOC Service Interruption Coordinator from Bell Nexxia. The request includes a list of several hundred circuit numbers, the maintenance date, a 4-hour window for the actual work, and an anticipated outage of 30 minutes within this window.
2. Using JNDMS, the Service Interruption Coordinator copies the circuit list into a query table and obtains a report of the services using these circuits, the locations affected, and the operations using those services now, and scheduled to be using them in 30 days. The Service Interruption Coordinator observes that a critical system required for a scheduled operation will be affected. The Service Interruption Coordinator contacts Bell Nexxia and requests that the maintenance be scheduled for another time period.
3. Bell Nexxia escalates the need for this maintenance to occur at the initially proposed time due to the number of people involved and the impossibility of finding another time that will accommodate everyone. The cost of changing the maintenance time is estimated at several million dollars.
4. The Service Interruption Coordinator informs the chain of command about this dilemma. The decision is escalated to J6 who decides after confirming the JNDMS information with the Command Centre that the operational requirement for the systems cannot be changed and that DND cannot accept, regardless of the cost, the proposed maintenance time.
5. Using JNDMS to forecast periods when the operational impact will be minimized, the Service Interruption Coordinator provides a list of alternate time intervals. Bell Nexxia presents this list to its other clients and one of the intervals on the list is accepted.

7.8 Scenario 8 - Provide Network Infrastructure Data

Objective: To populate the JNDMS Data Store with Static IT Infrastructure Data and their Location, and display the information to the JNDMS user.

Use Case(s) Addressed:

- Acquire IT Infrastructure Data
- Pre-process IT Infrastructure Data
- Store IT Infrastructure Data
- Role-based and User-defined Views

Background: JNDMS has just been installed on a new DND network. In order to commence displaying SA for this network the static IT Infrastructure Data and location information must be acquired, pre-processed and stored in the JNDMS Data Store.

Scope: Regional

Configuration and Preconditions:

A fully operational DND network is available or simulated. There is no network data available in the JNDMS Data Store.

Roles and Tasks:

System Administrator

Sequence of Activities:

1. The system administrator logs into the JNDMS and the system is started.
2. The static IT Infrastructure data and location information is acquired from the network management tool responsible for the baseline.

In Cycle 1:

- Since the CMDB is not captured in a network management tool, EIM will simulate the baseline data by doing a network discovery and populating its database. This data will be transferred into the JNDMS Data Warehouse.
- A few SDAs will be created in the Data Warehouse, along with their locations (approximated latitude and longitude).
- A few DWAN routers will be created and assigned to an existing SDA.
- A few services and their servers will be created and assigned to an existing SDA.
- Relationships between the routers, servers and services will be captured in the Data Warehouse.

3. The Static IT infrastructure data and location information is pre-processed for storage in the JNDMS Data Store.
4. The Static IT infrastructure data and location information is stored in the JNDMS Data Store.
5. The Static data and location information is displayed on the JNDMS through the Geospatial Information System (GIS), presenting different logical inter-connectivity schematics/diagram.
6. When the IT infrastructure baseline is updated, JNDMS receives the updated data from the CMDB.

In cycle 1, the updated baseline data will be received from EIM as an “Updated Baseline” event.

7.9 Scenario 9 – NSM Discovers and Monitors the Devices on the Network

Objective: To identify new, updated, removed or failed devices on the monitored network.

Use Case(s) Addressed:

Background:

The NSM component of EIM provides continuous discovery of network devices and availability monitoring of those devices. The monitored network is using DHCP to provide the IP address for user workstations.

The following events will be demonstrated:

- New devices are discovered and evaluated as to whether they are rogue or new assets,
- Missing assets are identified and evaluated as to why they are off-line.

Scope:

Regional

Configuration and Preconditions:

Single Network with single JNDMS instance

Roles and Tasks:

Sequence of Activities:

1. The JNDMS system is operating.
2. The NSM Continuous Discovery identifies a new device.
3. The NSM Continuous Discovery sends a “New Device Found” event to the NSM Event management component, which will in turn push the event to JNDMS.
4. The JNDMS DSS analyzes the event and engages the workflow to highlight the introduction of a new device in the network. The new device will be displayed with a blue color (blue items represent “Other Incident”) until it is reviewed and added to the baseline.
5. Rogue asset events are ranked according to the risk they pose to the mission. For approved assets the JNDMS infrastructure baseline is updated.
6. The IP on a workstation on the monitored network is changed.

7. The NSM Continuous Discovery detects the change in the workstation's IP.
8. The NSM Continuous Discovery sends an "IP address changed" event to the NSM Event management component, which pushes the event to JNDMS.
9. The JNDMS DSS analyzes the event and engages the workflow to decide if this address change is acceptable or not. Until this event is resolved, the workstation is represented with a blue circle (Other Incident).
10. Once the change has been reviewed and approved, the JNDMS infrastructure baseline is updated.
11. The NSM Distributed State Machine, through its continuous monitoring, detects that a known device fails to answer to its regular polling.
12. The NSM Distributed State Machine sends a "Device Down" event to the NSM Event management component, which pushes the event to JNDMS.
13. The JNDMS DSS analyzes the event and engages the workflow to investigate why the device is not responding any more. The workstation is displayed with a red circle (Outage).
14. The DSS performs a severity assessment to highlight the impact of this event. If the device was authorized for removal from the network the JNDMS infrastructure baseline will be updated to reflect that removal and any incident or vulnerability instance related to the device is closed.

7.10 Scenario 10 - SIM Collects the Security Events

Objective: To populate the JNDMS Data Store information on security events and display the information to the JNDMS user.

Use Case(s) Addressed:

- Acquire Security Events
- Pre-Process Security Events
- Store Incidents
- Role-based and User-defined Views

Background:

A JNDMS is deployed on an Intranet connected network for the purposes of providing SA of that CND environment. SIM is used to acquire security data from the CND environment. This scenario will be used as the overriding scenario for a series of smaller (sub) scenarios dealing with specific Security events

Scope: Regional

Configuration and Preconditions: TBD

Roles and Tasks: TBD

Sequence of Activities:

The following sequence of activities is generic/general for most events. The individual sub scenarios may either include additional activities or may not include a specific activity listed.

1. A Security Event is detected by an IDS or reported by an external source.
2. The effects of the Security Event are detected by EIM or reported by an external source.
3. After data acquisition, SIM processes each kind of alert by storing it in the SDW and sending either aggregated or atomic (single event) data through its rules engine. Those events above the threshold of importance are forwarded on to JNDMS through the web services.
4. The DSS attempts to correlate the ISM events with other known events, and performs severity assessments.
5. Situational Awareness overview and Defensive Posture are updated.

Sub Scenarios

Asset targeted by Denial of Service Attack

Synopsis: A DoS attack targeting a web server is detected. Shortly thereafter EIM detects the web server is offline.

Objective: Show correlation between SIM and EIM.

Background: A web server at a monitored site is targeted with a “land” attack packet (Vul 4) from an attacker.

This event is detected by IDS (Sig 1) and reported through the SIM to JNDMS. No corresponding vulnerability instance is associated with the web server.

Shortly thereafter the web server stops responding to solicitations from the EIM and a “Status Down” message is sent to JNDMS.

Exploits are detected targeting two assets

Synopsis: An IDS detects two identical exploits targeting two different assets. One of the assets is not vulnerable (based on CVE match), not critical to the mission, does not contain sensitive information.

Objective: Show “environmental” correlation – rules which contextualize and rank events based on CND knowledge.

Background: Two database servers at a monitored site are targeted by an attacker infected with the Slammer worm.

These events are detected by IDS (Sig 2) and reported through the SIM to JNDMS. One database server is vulnerable (Vuln 1) the other is not.

Exploits are detected targeting two zones

Synopsis: An IDS detects two identical exploits targeting two similar assets in two different zones. The system calculates that the vectoring safeguards are likely effective at the perimeter of one zone and not effective for the other zone.

Objective: Demonstrate zoning concept of vectoring safeguards.

Background: A web server at one monitored Site (site 1) and a web server at a second monitored site (site 2) in close proximity are targeted by an attacker using a Code Red variant (Vul 2). This is detected by IDS (Sig 3) and reported to JNDMS.

Evidence of compromise detected

Synopsis: An IDS detects evidence of a successful compromise on an internal asset. Damage/Impact are calculated in the context of the mission.

Objective: Highlight the difference between evidence of attack (attempt) and evidence of damage (actual impact).

Background: An IDS detects (Sig 4) a workstation infected with the “sars notifier” Trojan (Malware 1)

External report of damage investigated

Synopsis: A user calls to report what they believe to be the compromise of their machine. An analyst uses JNDMS to record the incident, start the investigation and assess mission impact.

Objective: Show ability of system to calculate and factor in relevant data for which there are no sensors.

Background: A user calls the Help Desk to report a malware infection on their workstation. The malware type, possible vulnerability and attacker are unknown.

Security incident is escalated by Analyst

Synopsis: An incident affecting an asset targeted by an exploit which is under investigation in the system is upgraded from “system attacked” to “system compromised” by an Analyst.

Objective: Show how ongoing incidents will change and how this affects SA/Defensive Posture.

Background: A database server at a monitored site is under investigation due to a prior exploit attempt (see sub scenario - Exploits are detected targeting two assets). After the analyst inspects the packet logs in Shadow then logs on to the machine, the analyst determines it is compromised, and upgrades the incident in JNDMS accordingly.

Asset targeted by exploit becomes source of exploit

Synopsis: A database server exposed to the Internet in the DMZ is the target of an exploit. Shortly thereafter the same server is the source of an exploit targeting a database server on the internal network.

Objective: Show “environmental aware” correlation across multiple assets/topography.

Background: A database server in a monitored site DMZ is targeted by an attacker infected with the Slammer worm.

These events are detected by IDS (Sig 2) and reported through the SIM to JNDMS. The database server is vulnerable (Vuln 7) to the attack.

Shortly thereafter the database server in the DMZ is detected by IDS (Sig 2) to be attacking an internal DB server at the same site.

All assets at two locations stop responding

Synopsis: EIM detects that all assets at two physical locations have stopped responding. Information Security products report relevant events associated with the assets in question. No other locations report outages.

Objective: Show the value of the geospatial view – allow correlation by human analyst.

Background: All assets at two sites in close physical proximity stop responding to solicitations from the EIM.

A Geospatial view shows the outages in the context of the Op Area. This reveals the affected locations are ion close physical proximity.

7.11 Scenario 11 - Provide Military Operations Data

Objective:

1. To populate the JNDMS Data Store with information on a specified military operation and display the information to the JNDMS user.
2. To provide partial replication of data between two different JNDMS instances.

Use Case(s) Addressed: (Model may need new high level use case diagram for this scenario)

- Acquire Military Operations Data
- Pre-Process Operations Data
- Store Operations Data
- Role-based and User-defined Views

Background:

The DCDS has issued a tasking to the Commander of Joint Task Force Atlantic (JTFA) to conduct operations in support of enforcing UN embargos against an unsavoury Republic which is currently involved in a particularly gruesome Civil War. Both sides are relying on illegal drug exports to fund their efforts. JTFA will be operating within Coalition to prevent either side from exporting their illegal drugs.

JNDMS is fitted at both the NDHQ and JTFA NOCs.

Scope: International

Configuration and Preconditions:

Two functional JNDMS on separate networks (This configuration cannot be tested during Cycle 1.)

Roles and Tasks: TBD

Sequence of Activities:

1. JTFA and NDHQ NOCs are sharing their static IT Infrastructure Data at the main router and server levels. Data synchronization between the two sites is hourly.
2. Both sites acquire, pre-process and store the available operational data.

Cycle 1:

- A few operations will be simulated and entered directly into the JNDMS Data Warehouse. These operations will use services already simulated in the IT infrastructure data.

3. The operational data is available for display in both JNDMS.

7.12 Scenario 12- NVAT is Informed of a New Vulnerability

Objective: To populate the JNDMS Data Store with vulnerability data and display the information to the JNDMS user.

Use Case(s) Addressed:

- Acquire Vulnerability and Exploit Data
- Pre-Process Vulnerability and Exploit Data
- Store Vulnerability and Exploit Data
- Role-based and User-defined Views

Background:

The JNDMS is operating on a Network. The vulnerability analyst has been informed of a new vulnerability and must determine if the network is affected by this vulnerability. The vulnerability analyst has also been tasked to determine the vulnerabilities of the network and develop a plan to address them. This scenario will be used as the overriding scenario for a series of smaller (sub) scenarios dealing with specific sources of vulnerability data.

Scope: Regional

Configuration and Preconditions: TBD

Roles and Tasks:

Vulnerability Analyst

Sequence of Activities:

1. The vulnerability analyst acquires vulnerability definitions from a public online source (the National Vulnerability Database [NVD]), or
 - The vulnerability analyst receives an intelligence report about a new vulnerability.
 - The analyst verifies if JNDMS is aware of this vulnerability. The vulnerability is not yet available in JNDMS or
 - A new vulnerability is detected.
2. The analyst enters this vulnerability into the Impact Assessment Tool (IAT) and the new vulnerability is pushed to JNDMS.
3. The DSS queries the JNDMS Data Warehouse for devices that are vulnerable to the new vulnerability definition.
4. JNDMS creates a vulnerability instance for each vulnerable device and stores it in the Data Warehouse.

5. DSS performs risk assessments for each new vulnerability instance.
6. The vulnerability analyst can see the results in the security view. The new vulnerability instances are displayed in the vulnerability table, as well as on the GIS view, if applicable.

Sub Scenarios

A new vulnerability is disclosed

Synopsis: A new vulnerability definition is loaded into the system. The system calculates vulnerability instances based on the asset CMDB. The new threat to the mission is assessed based on mission impact.

Objective: Demonstrate proposed approach to vulnerability disclosure. Accommodate common NVAT use case.

Background: A new vulnerability is disclosed (Vuln 3) through NVD and loaded in JNDMS. A CMDB query reveals that a web server in a monitored site is running a vulnerable version of the software.

A vulnerability is updated

Synopsis: A vulnerability definition already in the system is updated by a JNDMS analyst to reflect new information which changes the severity of the vulnerability (a worm exploiting the vulnerability has been detected in the wild). The system recalculates the threat to the mission.

Objective: Accommodate common NVAT use case.

Background: A worm exploiting a recent vulnerability (Vuln 3) is discovered in the wild (see A new vulnerability is disclosed). The web server identified in “**A new vulnerability is disclosed**” is exposed and vulnerable.

A “zero day” exploit is discovered in the wild

Synopsis: A new threat is detected in the form of exploit code targeting an undisclosed vulnerability in software commonly used in the CND environment. The threat is entered into the system (as a vulnerability). The system then calculates vulnerability instances and mission impact as per “**A new vulnerability is disclosed**”

Objective: Accommodate common NVAT use case.

Background: A zero day exploit (Malware 2) is discovered in the wild which appears to affect at minimum Win2K and WinXP. No CVE, patches or IDS signatures exist.

Scanner reveals vulnerabilities in assets

Synopsis: A Nessus scan result of assets is loaded into the system. The system calculates the differences since the last scan (reconciliation) and updates the JDW appropriately.

Objective: Accommodate common NVAT use case. No reconciliation with CMDB query generated vulnerabilities is required or desirable.

Background: .

The Asset CMDB is updated

Synopsis: A new extract of asset CMDB data is loaded into the system containing changes from the current (baseline) CMDB data. Changes to assets which affect Situational Awareness overview and Defensive Posture include:

- Assets are added/ removed
- Software is installed/ uninstalled/ upgraded (Normalized Product Version)
- A Patch is applied (against a vulnerability instance)
- An asset moves geographic location
- An asset moves logical/ network location (topology/ zone change)
 - Asset trust/ hostility value changes
- An asset is associated/ dissociated with an operation
- Confidentiality/ Integrity/ Availability value of an asset change
 - Criticality/ Sensitivity/ Availability Service Level Agreement changes
- Safeguards on the asset are updated.

Objective: Demonstrate approach to CMDB problem – externalizes issue of UAM product names and issue of (theoretical) externally managed asset CMDB.

Background: .

New virus detected in detected in the wild

Synopsis: A new phishing email tricks users into visiting a malicious website to download a trojan. No "CVE" vulnerability is involved - it is a social engineering attack to trick recipients of the email into running malicious code on the internal network. Information about this new threat (Distribution: High, Damage: High, various details) is loaded into the system via a feed and/ or updated by hand.

Objective: Accommodate common NVAT use case.

Background:

7.13 Scenario 13 - Provide Safeguard Data

Objective: To populate the JNDMS Data Store with the configuration of safeguard data and display the information to the JNDMS user

Use Case(s) Addressed:

- Identify Safeguard Data
- Pre-Process Safeguard Data
- Store Safeguard Data
- Role-based and User-defined Views

Background:

JNDMS captures the configuration of the network safeguards. These include the firewall rules and the router's Access Control Lists.

Scope:

The firewall rules and ACLs will be described to JNDMS through the manual configuration of the safeguards. The rules and ACLs will not be automatically discovered.

Configuration and Preconditions:

Roles and Tasks:

Sequence of Activities:

1. The ISSO acquires safeguard data

Cycle 1:

- This configuration data is simulated and stored directly into the JNDMS Data Warehouse.
- 2. The safeguard data is pre-processed.
- 3. The safeguard data is stored in the appropriate JNDMS Data Store.
- 4. The safeguard data is displayed to the user in the Defensive Posture view. The user can access the configuration of the safeguard by double-clicking on the safeguard.

7.14 Scenario 14 - Multi-Level Security Domains

Objective: JNDMS to provide for exchange of data using a one-way transfer media for Multi-Level classification domains

Use Case(s) Addressed:

- Exchange data across classification layer

Background:

A NOC is responsible for monitoring the performance and status for both Protected A and Secret level networks in a metropolitan area. The NOC has separate instances of JNDMS on each of the security domains. The JNDMS in the Secret domain is monitored 24/7, while the JNDMS in the Protected A domain is monitored 8/5. To provide support for the Protected A network during the silent hours and weekend, the Protected A JNDMS provides IT Infrastructure data to the main servers and router level to the Secret level JNDMS. Additionally, all events/incidents above a predetermined level on the Protected A network are transferred to the Secret network JNDMS.

Scope: National

Configuration and Preconditions:

Secret level network with JNDMS instance (may be simulated)

Protected A level network with JNDMS instance (may be simulated)

Roles and Tasks: TBD

Sequence of Activities:

1. Both Network JNDMS instances are set up and running correctly.
2. The Protected A network JNDMS is configured to transfer static IT Infrastructure data for the networks main servers and routers to the Secret network JNDMS.
3. The Protected A network JNDMS is configured to transfer all Protected A incidents to the Secret network JNDMS in near real-time.
4. The Protected A network JNDMS is not being monitored.
5. Create incidents on the Protected A network.
6. Monitor the Secret level JNDMS. DSS performs severity assessments. The user can take appropriate action on reported security incidents severities.

ANNEX A - EXPERIMENTS

The JNDMS Experiment Reports will constitute Annex A to this document. Each Experiment Report will be issued as a stand-alone document.

ANNEX B – TRIALS

The JNDMS Trials Reports will constitute Annex A to this document. Each Trial Report will be issued as a stand-alone document.

ANNEX C – DEMONSTRATIONS

A JNDMS Demonstration Plan will be created for each scheduled formal demonstration. Each Demonstration Plan will be issued as a stand-alone document.